AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of determining network penetration, the method comprising the computer-implemented steps of:

receiving first information that identifies a packet;

representing a possible travel of [[a]] the packet in a network based on topology data and on security policy data;

wherein the step of representing comprises:

checking the first information against an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet, wherein checking the first information against the inbound ACL includes determining whether the inbound ACL permits ingress of the packet at the network device;

if the inbound ACL permits the ingress of the packet at the network device, checking the first information against one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the network device;

checking the topology data to determine one or more neighbor network devices that the packet could reach, wherein the one or more neighbor network devices are respectively connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

~~for each of the one or more possible outbound interfaces on which the egress of~~

~~the packet is permitted,~~ repeating the checking steps ~~with respect to~~ for each neighbor network device, of the one or more neighbor network devices, that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing, wherein the output comprises second information that specifies one or more of: possible paths that the packet could take in the network, and a set of network devices that the packet could reach in the network;

wherein the steps of the method are performed by one or more computer systems.

2. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the security policy data comprises one or more access control lists of one or more network devices in the network.

3. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, ~~further comprising the step of receiving~~ wherein the first information comprises packet parameters.

4. (Currently Amended) ~~A method as recited in~~ The method of Claim 3, wherein the packet parameters comprise an identifier of the network entry point where the packet enters the network.

5. (Currently Amended) ~~A method as recited in~~ The method of Claim 3, wherein the

packet parameters comprise a destination address.

6. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the topology data is received as input related to a user interface.

7. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the security policy data is based on access control lists associated with input received in a user interface.

8. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the step of representing further comprisinges determining a maximum penetration point.

9. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the step of representing comprises accessing the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach.

10. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the step of representing comprises determining whether ingress is allowed to a neighbor network device for which it has been determined that ~~the inbound interface~~ could be reached by the packet.

11. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the step of representing comprises determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet

could reach.

12. (Currently Amended) ~~A method as recited in~~ The method of Claim 1, wherein the step of representing comprises determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

13. (Currently Amended) ~~A method as recited in~~ The method of Claim 12, wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces.

14. (Canceled)

15. (Currently Amended) ~~A method as recited in c~~ The method of Claim 1, further comprising receiving third information that specifies packet parameters ~~specifying information~~ corresponding to a plurality of different packets.

16. (Currently Amended) ~~A method as recited in c~~ The method of Claim 1, wherein the step of representing comprises:

for a neighbor network device for which it is determined that the packet could reach,

determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet from the neighbor network device is permitted based on the static routing table.

17. (Currently Amended) The method of ~~c~~Claim 16, further comprising not considering any outbound interface through which egress of the packet is permitted by the static routing table but is not permitted by an access control list associated with the security policy data.

18. (Currently Amended) ~~A method as recited in c~~ The method of Claim 1, wherein the step of representing comprises:

for a neighbor network device for which it is determined that the packet could reach, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the possible travel of the packet.

19. (Currently Amended) ~~A method as recited in c~~ The method of Claim 1, wherein the step of receiving the first information further comprises receiving packet parameters that support transmission control protocol flags.

20. (Currently Amended) ~~A method as recited in c~~ The method of Claim 1, wherein the ~~results~~ output comprises a graphical display of at least ~~allowed paths of the packet~~ the second information.

21. (Currently Amended) ~~A method as recited in c~~ The method of Claim 19, wherein the graphical display also includes at least a mapping of the set of network devices and connections between the network devices in the set of network devices.

22. (Currently Amended) A method of determining potential penetration of ~~a~~ packets into a network, the method comprising the computer-implemented steps of:

receiving network topology data;

receiving first information defining a packet flow comprising a source address;

receiving second information defining a first network device, comprising a network address and an ingress interface identifier for an ingress interface of the first network device;

determining whether the ingress interface of the first network device allows the packet flow to enter the first network device, based on checking the first information against a first access control list associated with the ingress interface;

determining one or more egress interfaces of the first network device that allow egress of the packet flow from the first network device, based on checking the first information against one or more second access control lists associated with the one or more egress interfaces;

based on the network topology data, determining one or more second network devices that are coupled to the one or more egress interfaces; and

recursively performing the determining steps for each of the one or more second network devices;

wherein the steps of the method are performed by one or more computer systems.

23. (Currently Amended) ~~A method as recited in~~ The method of Claim 22, further comprising the step[[s]] of determining if a static routing table is present for the first network device, and wherein the step of determining the one or more egress interfaces ~~is performed based on~~ further comprises checking the first information against the static

routing table.

24. (Currently Amended) The method of ~~e~~Claim 23, further comprising not considering an ~~outbound~~ egress interface through which egress of the packet flow is permitted by the static routing table but is not permitted by the one or more second access control lists.

25. (Currently Amended) A method of determining network penetration, the method comprising the computer-implemented steps of:

representing a travel of a packet in a network based on topology data and on security policy data including at least the steps of:

receiving first information that defin~~inge~~s a packet by at least specifying a source address for the packet ~~, an entry port, and a destination port~~ and an entry point that identifies a current network device in the network;

starting a loop for [[a]] the current network device;

accessing access control lists (ACLs) in the security policy data stored in an ACL database and the topology data stored in a topology database;

deciding whether an ingress interface of [[a]] the current network device allows entry of the packet into the current network device by checking the first information against an inbound ACL, from the security policy data, that is associated with the ingress interface of the current network device, wherein:

if the entry is not permitted, then terminating the loop for the current network device[[,]];

if the entry is permitted, then ~~performing the steps of:~~

checking the first information against one or more outbound ACLs, from the security policy data, for each outbound interface of the current network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the current network device;

~~continuing the loop;~~

determining if a static routing table is present for the current network device, wherein:

if the static routing table is present then determining ~~to~~ from which outbound interface outbound traffic is permitted to exit the current network device[[,]]; and

if the static routing table is not present, then determining that the outbound traffic is allowed to exit through all outbound interfaces of the current network device;

based on the topology data, determining if there are any neighboring network devices that are connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the current network device, wherein:

if there are not any neighboring network devices, then returning an indication of the current network device as a maximum penetration point as at least part of results of the step of representing, and terminating the loop for the current network device;

~~if there is at least one neighboring network device, then continuing the~~

~~loop;~~

determining whether or not there are any remaining possible outbound interfaces for which results of a possible egress of the packet have not been determined, wherein:

if there are no more remaining possible outbound interfaces, then terminating the loop for the current network device[[,]];

if there are more remaining possible outbound interfaces, then setting the current network device to a neighboring network device that corresponds to one of the remaining possible outbound interfaces[[,]]; and

if the loop has not been terminated ~~for the current network device~~, then restarting the loop for the current network device;

wherein the steps of the method are performed by one or more computer systems.

26. (Currently Amended) An apparatus for determining penetration into a network, the apparatus comprising:

one or more processors;

a topology database storing topology information about the network;

an Access Control List (ACL) database storing ACLs ~~information~~ related to the network;

a non-transitory computer-readable storage medium storing one or more sequences of instructions that comprise instructions for displaying a penetration Graphical User Interface (GUI) including at least:

input fields having at least:

~~a topology information input field,~~

~~an ACL input field,~~

a source address input field for ~~entering~~ receiving at least a source address of a packet, and

an entry point field for ~~entering~~ receiving at least one entry point to the network for the packet~~, and~~

~~a destination input field for entering at least a destination address for the packet~~; and

output penetration information fields for a graphical output including:

network devices of the network,

connections between the network devices corresponding to the topology information ~~data~~,

at least one entry point to the network,

paths the packet is allowed to follow based on the topology ~~data~~ information and the ACLs ~~data~~, and

at least one maximum penetration point; and

a penetration module configured to:

access the topology database to retrieve the topology information;

access the ACL database to retrieve the ACLs;

receive input corresponding to the input fields;

check the source address of the packet, specified in the source address input field, against an inbound ACL of an interface of a network device specified ~~by the input~~ in the entry point field;

if the inbound ACL permits ingress of the packet at the network device, check

the source address of the packet against one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the network device;

check the topology information to determine one or more neighbor network devices that the packet could reach, wherein the one or more neighbor network devices are respectively connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

repeat the checks for each neighbor network device, of the one or more neighbor network devices, that is connected to each of the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device; and

produce ~~the output penetration information~~ the graphical output for display in the penetration GUI.

27. (Currently Amended) An apparatus for determining network penetration, the apparatus comprising:

one or more processors, and a non-transitory computer-readable storage medium storing one or more sequences of instructions that comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving first information that identifies a packet;

representing a possible travel of [[a]] the packet in a network based on topology

data and on security policy data;

wherein the step of representing comprises:

checking the first information against an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet, wherein checking the first information against the inbound ACL includes determining whether the inbound ACL permits ingress of the packet at the network device;

if the inbound ACL permits the ingress of the packet at the network device, checking the first information against one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the network device;

checking the topology data to determine one or more neighbor network devices that the packet could reach, wherein the one or more neighbor network devices are respectively connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

~~for each of the one or more possible outbound interfaces on which the egress of the packet is permitted,~~ repeating the checking steps ~~with respect to~~ for each neighbor network device, of the one or more neighbor network devices, that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the

network, based on the step of representing, wherein the output comprises second information that specifies one or more of: possible paths that the packet could take in the network, and a set of network devices that the packet could reach in the network.

28. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the security policy data comprises one or more access control lists stored on one or more network devices in the network.

29. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein ~~the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving~~ the first information comprises packet parameters.

30. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 29, wherein the packet parameters comprise an identifier of the network entry point where the packet enters the network.

31. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 29, wherein the packet parameters comprise a destination address.

32. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the topology data is based on input related to a user interface.

33. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein

the security policy data is based on access control lists associated with input related to a user interface.

34. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the ~~one or more sequences of~~ instructions that cause the one or more processors to perform the step of representing further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining a maximum penetration point.

35. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of accessing the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach.

36. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether ingress is allowed to a neighbor network device ~~whose inbound interface~~ for which it has been determined that the packet could reach.

37. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein

the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could reach.

38. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

39. (Currently Amended) ~~An apparatus as recited in~~ The apparatus of Claim 38, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of recursively applying the step of determining whether there are any outbound interfaces.

40. (Canceled)

41. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform

the step of receiving third information that specifies ~~wherein the~~ packet parameters ~~specify information~~ corresponding to a plurality of different packets.

42. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

for a neighbor network device being represented as having been reached by the packet,

determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet from the neighbor network device is permitted based on the static routing table.

43. (Currently Amended) ~~An~~ The apparatus of ~~c~~Claim 42, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of not considering any outbound interface through which egress of the packet is permitted by the static routing table but is not permitted by an access control list associated with the security policy data.

44. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more

processors, cause the one or more processors to perform the steps of:

for a neighbor network device for which it is determined that the packet could reach,

determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the possible travel of the packet.

45. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the ~~one or more sequences of~~ instructions that cause the one or more processors to perform the step of receiving the first information further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters that support transmission control protocol flags.

46. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the ~~results~~ output comprises a graphical display of at least ~~allowed paths of the packet~~ the second information.

47. (Currently Amended) ~~An apparatus as recited in c~~ The apparatus of Claim 27, wherein the graphical display also includes at least a mapping of the set of network devices and connections between the network devices in the set of network devices.

48. (Canceled)

49. (Currently Amended) A non-transitory computer-readable storage medium storing one

or more sequences of instructions that comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving first information that identifies a packet;

representing a possible travel of [[a]] the packet in a network based on topology data and on security policy data;

wherein the step of representing comprises:

checking the first information against an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet, wherein checking the first information against the inbound ACL includes determining whether the inbound ACL permits ingress of the packet at the network device;

if the inbound ACL permits the ingress of the packet at the network device, checking the first information against one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the network device;

checking the topology data to determine one or more neighbor network devices that the packet could reach, wherein the one or more neighbor network devices are respectively connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

~~for each of the one or more possible outbound interfaces on which the egress of the packet is permitted,~~ repeating the checking steps ~~with respect to~~ for each neighbor network device, of the one or more neighbor network

devices, that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing, wherein the output comprises second information that specifies one or more of: possible paths that the packet could take in the network, and a set of network devices that the packet could reach in the network.

50. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the security policy data comprises one or more access control lists of one or more network devices in the network.

51. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein ~~the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving~~ the first information comprises packet parameters.

52. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 51, wherein the packet parameters comprise an identifier of the network entry point where the packet enters the network.

53. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 51, wherein the packet parameters comprise a destination address.

54. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim ~~51~~ 49, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of reading the topology ~~information~~ data from a topology database.

55. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the topology data is based on input related to a user interface.

56. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the security policy data is based on access control lists associated with input related to a user interface.

57. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the ~~one or more sequences of~~ instructions that cause the one or more processors to perform the step of representing further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining a maximum penetration point.

58. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of accessing

the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach.

59. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether ingress is allowed to a neighbor network device ~~whose inbound interface~~ for which it has been determined that the packet could reach.

60. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could reach.

61. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any possible outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

62. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim [[49]] 61, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of recursively applying the step of determining whether there are any outbound interfaces.

63. (Canceled)

64. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving third information that specifies packet parameters ~~specifying information~~ corresponding to a plurality of different packets.

65. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

for a neighbor network device that could be reached by the packet, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet from the neighbor network device is permitted based on the static routing table.

66. (Currently Amended) [[A]] The non-transitory computer-readable storage medium of ~~e~~Claim 65, wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of not considering any outbound interface through which egress of the packet is permitted by the static routing table but is not permitted by an access control list associated with the security policy data.

67. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim ~~51~~ 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

for a neighbor network device that could be reached by the packet, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the possible travel of the packet.

68. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim ~~51~~ 49, wherein the ~~one or more sequences of~~ instructions that cause the one or more processors to perform the step of receiving the first information further comprise instructions which, when executed by the one or more processors, cause the

one or more processors to perform the step of receiving packet parameters that support transmission control protocol flags.

69. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim ~~51~~ 49, wherein the ~~results~~ output comprises a graphical display of at least ~~allowed paths of the packet~~ the second information.

70. (Currently Amended) [[A]] The non-transitory computer-readable storage medium ~~as recited in~~ of Claim ~~69~~ 49, wherein the graphical display also includes at least a mapping of the set of network devices and connections between the network devices in the set of network devices.

71. (Canceled)

72. (Currently Amended) An apparatus for determining network penetration comprising:

means for receiving first information that identifies a packet;

means for representing a possible travel of [[a]] the packet in a network based on topology data and on security policy data;

wherein the means for representing comprise:

means for checking the first information against an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet, wherein the means for checking the first information against the inbound ACL include means for determining whether the inbound ACL permits ingress

of the packet at the network device;

means for checking the first information against one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted from the network device when the inbound ACL permits the ingress of the packet at the network device;

means for checking the topology data to determine one or more neighbor network devices that the packet could reach, wherein the one or more neighbor network devices are respectively connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

means for repeatedly invoking the means for checking the first information against the inbound ACL, ~~and~~ the means for checking the first information against the one or more outbound ACLs, and the means for checking the topology data ~~with respect to~~ for each neighbor network device, of the one or more neighbor network devices, that is connected to each of the one or more possible outbound interfaces on which the egress of the packet is permitted from the network device;

means for providing ~~an~~ penetration output that specifies a possible penetration of the packet into the network, based on output from the means for representing, wherein the penetration output comprises second information that specifies one or more of: possible paths that the packet could take in the network, and a set of network devices that the packet could reach in the network.